PERFORMING CYBERSECURITY EXPERTISE: CHALLENGES FOR PUBLIC UTILITY COMMISSIONS

Rebecca Slayton†

ABSTRACT

Regulators have evolved organizational processes, capacities, and expertise that aim to balance public goods such as reliability, affordability, and environmental protection. However, cybersecurity is a different kind of good. It requires continual vigilance by experts and continual advancements in their practices as cybersecurity involves intelligent adversaries that seek to undermine it. Regulators have thus expressed concern that neither they nor the companies they regulate have the expertise to ensure that critical infrastructure remains uncompromised. This Article examines such expertise as an authoritative relationship between individuals claiming specialized skills and those without such training. In particular, it considers how public utility commissions help produce critical infrastructure cybersecurity expertise. It argues that the commissions have not merely accessed expertise but have worked with skilled individuals to actively produce expertise. The analysis highlights three contexts and processes for producing such expertise. First, after breaches occur in utility networks, commission experts highlight industry-accepted best practices and standards—not only to explain the breaches, but to emphasize that they possess specialized knowledge that could have prevented such breaches. Second, commission experts maintain ongoing discussions with utilities, such that utility requests for rate recovery associated with cybersecurity investments rarely need to be publicly challenged—a process which might reveal disagreement among experts and undermine authority. Third, when experts are called upon to help establish cybersecurity standards, they have attempted to remain neutral and facilitate agreement among industry experts. However, in the midst of public controversy about appropriate standards, regulators have at times struggled to maintain their authority.

DOI: https://doi.org/10.15779/Z380R9M47Q

† Rebecca Slayton is Associate Professor jointly in the Science & Technology Studies Department and Judith Reppy Institute for Peace and Conflict Studies, both at Cornell University. She is currently working on a book about the history of cybersecurity expertise. This paper is based upon research supported by the National Science Foundation under grant number 1553069.

TABLE OF CONTENTS

I. INTRODUCTION

In the past twenty years, growing dependence on cyberspace has made national security a concern of relatively small, subnational organizations ranging from private companies to provincial, state, and local governments. Small businesses with no obvious relation to national security have found themselves in the crosshairs of state-sponsored campaigns designed to infiltrate national critical infrastructure and undermine national security. A recent report revealed that Russian hackers infiltrated the U.S. electrical power grid by targeting tiny, seemingly insignificant contractors in at least twenty-four states, exploiting trust networks.[1] The hackers targeted at least sixty

1. Rebecca Smith & Rob Barry, *America's Electric Grid Has a Vulnerable Back Door - and Russia Walked Through It*, WALL ST. J. (Jan. 10, 2019, 11:18 AM), https://

utilities, breached about two dozen of them, and gained access to the control rooms of eight or more—where they could have turned off the power had they wished to do so.[2] This suggests a success rate of over ten percent, but the potential impact of such compromises is much greater because of complex interdependency in the electrical power grid, where relatively small local disturbances can cascade into much larger failures if not managed well.[3]

In this context, federal, state, and local regulators have all expressed anxiety about how they can ensure the security of critical utility infrastructures, such as the power grid.[4] Regulators have evolved organizational processes, capacities, and expertise that aim to balance public goods such as reliability, affordability, and environmental protection, but cybersecurity is a different kind of good. Whereas reliability and efficiency have traditionally been understood as relatively deterministic, predictable characteristics, security implies an intelligent adversary that seeks to undermine it. No technological fix can provide assurance of cybersecurity; it requires continual vigilance by experts and continual advancements in their practices and knowledge. Indeed, cybersecurity can be understood as a race between experts on opposite sides of the law; white hats seek to defend systems while black hats seek to compromise them.

Thus, regulators have expressed concern that neither they nor the companies they regulate have the expertise needed to ensure that critical infrastructure remains uncompromised. A recent article by public utility commissioners notes that "[a]s the range and specialization of cyber threats grow, it will become increasingly difficult for companies to maintain sufficient in-house expertise to detect and manage penetrations."[5] A working paper from

www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112.

2. *Id.*

3. *See* U.S.-CAN. POWER SYS. OUTAGE TASK FORCE, FINAL REPORT ON THE AUGUST 14, 2003 BLACKOUT IN THE UNITED STATES AND CANADA: CAUSES AND RECOMMENDATIONS (2004), https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf (discussing the source of the 2003 Northeast Blackout).

4. *See, e.g.*, MILES KEOGH & SHARON THOMAS, NAT'L ASS'N OF REGULATORY UTIL. COMM'RS, CYBERSECURITY: A PRIMER FOR STATE UTILITY REGULATORS VERSION 3.0 (2017), https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F; Lynne Holt & Mary Galligan, *State Public Utility Commissions' Role in Cybersecurity and Physical Security Issues: Trade-Offs and Challenges* (Pub. Utl. Research Ctr. at Univ. of Fla., Working Paper, Dec. 12, 2017), https://bear.warrington.ufl.edu/centers/purc/docs//papers/1707_STATE_PUC_ROLE_Cybersecurity_12_12_17.pdf.

5. Sherina Maye Edwards, Caitlin Shields, Anne McKeon & Nakhia Crossley, *Cybersecurity, Part II: Opportunities and Challenges for State Utility Regulators*, PUB. UTIL.

the Public Utilities Research Center similarly notes that commissions "face many of the same challenges as utilities in attracting and retaining employees with cybersecurity expertise," but must also "compete with utilities for skilled employees with the added disadvantage of inadequate state pay-scales."[6] Organizations such as the National Association of Regulatory Utility Commissioners (NARUC) recently created a cybersecurity primer with five steps for state utility regulators, starting with "[c]reate expertise within their own organizations" and pointing to training opportunities offered by NARUC and other organizations.[7] In short, a variety of studies have examined the question of how regulators can acquire expertise and have suggested training in-house employees, hiring new cybersecurity experts, contracting with external consultants, or some combination of all three.

This Article focuses on a related but distinct set of questions. What constitutes cybersecurity expertise in the context of critical infrastructure? How do regulators adjudicate between conflicting claims to expertise? And, given the frequency of breaches and the absence of any security guarantees, how is the authority of cybersecurity experts produced?

Addressing this broader set of problems requires theorizing *expertise*. As the brief discussion above suggests, most analyses of regulation implicitly define expertise in terms of specialized knowledge and skills that are possessed by individuals or groups of people. From this perspective, the primary challenge is to acquire objective and disinterested expertise, thereby enabling regulators to provide a check on private interests and ensure the provision of public goods.

A somewhat different conception of expertise has emerged from work in Science and Technology Studies (STS) and related fields such as anthropology, sociology, and history.[8] Scholars in these fields have argued that expertise should be understood as a set of relationships between experts, laypersons, and culturally valued objects of expertise—e.g., secure computer networks.[9] Thus, expertise entails more than the possession of specialized knowledge or

FORTNIGHTLY, (Mar. 2017), https://www.fortnightly.com/fortnightly/2017/03/cybersecurity-part-2.

6. HOLT & GALLIGAN, *supra* note 4, at 13.

7. KEOGH & THOMAS, *supra* note 4, at 20.

8. *See, e.g.*, Rebecca Slayton & Aaron Clark-Ginsberg, *Beyond Regulatory Capture: Coproducing Expertise for Critical Infrastructure Protection*, 12 REG. & GOVERNANCE 115 (2018). This review is heavily influenced by the framing of E. Summerson Carr*, Enactments of Expertise*, 39 ANN. REVS. ANTHROPOLOGY 17 (2010). For more on security expertise, see generally TRINE VILLUMSEN BERLING & CHRISTIAN BUEGER, SECURITY EXPERTISE: PRACTICE, POWER, RESPONSIBILITY (2015).

9. For an overview of this literature, see generally Carr, *supra* note 9.

skills by a group of people; it also entails a relationship between people who claim to possess specialized skills and those who do not. These relationships are constructed through several kinds of activities, including a process of training and socialization, wherein aspiring experts learn to "pass" as legitimate members of an expert culture; demonstrating intimacy and mastery over rare but culturally valued objects; authorizing experts through institutions such as professional certification bodies; and obscuring the contingency and incompleteness of expert evaluations through naturalization. Drawing on dramaturgical approaches to understanding everyday social interaction, STS scholars have argued that expert advice can be understood as a kind of performance; experts selectively highlight aspects of their work that enhance its authority while obscuring or minimizing uncertainties, disagreements, and other features that might undermine it.[10] Expertise thus entails more than possessing knowledge or skills. It entails persuading an audience of the veracity of specific claims and the effectiveness of particular actions.

In general, cybersecurity expertise is a tough act to perform. Institutional markers, such as certifications and college degrees, confer only limited authority. It is widely recognized that such markers are no guarantee of efficacy, and very prominent experts may have no credentials at all. Instead, cybersecurity experts gain authority by demonstrating mastery over culturally valued objects—computers, networks, and the data flowing through them—the details of which seem arcane to the average person. However, this is often a perverse kind of mastery: breaking into systems that are believed to be secure. Furthermore, cybersecurity experts do not promise that they can prevent all breaches. Cybersecurity experts agree that virtually all practical computer systems can be breached by a sufficiently determined adversary. Furthermore, since breaches may remain hidden for years at a time, and there are no comprehensive metrics with which to gauge the security of a system, cybersecurity experts can never be certain that a system has not already been breached. This offers a limited basis for demonstrating expertise.

All of this raises the question of how regulators know what experts to trust. Moreover, because improvements in security often entail tradeoffs with other public goods, regulators must often negotiate between different and conflicting kinds of expertise. The NARUC primer notes the need for "a nimble and complex balance of security, functionality, and cost," pointing out that "a 'perfect' defense against cyberattacks has a cost that may, and often does, outweigh the value of the information it protects . . . . [T]he energy sector

10. *See, e.g.*, STEPHEN HILGARTNER, SCIENCE ON STAGE: EXPERT ADVICE AS PUBLIC DRAMA (2000).

cannot expect to 'gold plate' the grid."[11] Crucially, the logics that drive cybersecurity investments may be at odds with the logics grounding traditional investments in critical infrastructure. For example, as discussed further below, cybersecurity experts often invoke the need to keep pace with ever-changing threats—a need that can drive endless technological change and associated expense. However, this conflicts quite directly with regulators' goal of keeping rates associated with public goods such as electricity, gas, and water affordable and stable. Deciding what specific actions are appropriate thus requires both knowledge of technologies and practices used for security and value judgments about the relative importance of multiple goals.

How then, do regulators assure themselves and the public that they have achieved an appropriate balance between cybersecurity and other public goods? This paper argues that regulators have not merely accessed expertise but also worked with skilled and knowledgeable individuals to actively produce expertise. These findings have relevance not only for the cybersecurity of the electrical power grid, but for studies of regulation in complex technological industries more broadly.

The remainder of this Article consists of four main parts and a conclusion. The first overviews regulation for electrical grid cybersecurity, discussing how the grid became vulnerable to cyberattack, how federal regulators responded to these vulnerabilities, and how one state regulatory organization—the New York Public Services Commission (NYPSC or "Commission")—began to organize security expertise after the terrorist attacks of September 11, 2001.

The next three sections discuss three specific contexts in which the Commission's security experts have performed their expertise. First, Commission staff have been called upon to assess security in the wake of breaches. Although a security breach effectively means that experts working against the law have gotten the best of experts attempting to secure systems, there is little evidence that security breaches at utilities have undermined the public authority of either the utilities' or the Commission's security experts. Instead, the Commission's experts have responded to such breaches by identifying failures in the utilities' security practices, often with the help of consulting companies hired by the utilities. In so doing, the breaches have ironically reinforced the authority of cybersecurity experts by emphasizing that breaches are avoidable if organizations simply follow the best practices established by experts.

Second, the Commission's staff are often called upon to assess utilities' requests for rate recovery. These requests have grown, not only in response to

11. KEOGH & THOMAS, *supra* note 4, at 20.

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) requirements, but also in response to perceptions of rapidly evolving threats. It is here that the cooperative relationship between the Commission's experts and the utilities experts seems more apparent, for I have yet to find any example of the Commission staff criticizing or rejecting security initiatives proposed by utilities. This is not to suggest that any specific proposals should have been rejected. Rather, ongoing conversation among the utilities and the Commission's staff likely produces a high degree of convergence before rate cases are filed. The readiness of the Commission's staff to embrace arguments about perpetually evolving threats stands in contrast to the approach taken by regulatory experts in other states. I present one example from a similar rate case in Massachusetts.

And third, the Commission's staff has been called upon to help establish cybersecurity standards for smart grids. This is perhaps the most challenging site for performing expertise, because competition among a growing number of actors in electricity markets has led to conflict over appropriate standards of security. Although the Commission's staff attempted to defer to industry experts and a business-to-business process, they were not able to completely stay out of the fray.

II. THE ORIGINS OF POWER GRID CYBERSECURITY REGULATION

A. MAKING THE GRID "SMART"—AND VULNERABLE

The grid's vulnerability to cyberattacks has emerged as part of a broader shift in ways of producing, selling, and using electrical power. In the late 1980s and early 1990s, engineers and entrepreneurs began to contend that microprocessors and computer networking would enable free-market solutions to many problems. For example, utilities were increasingly wary of investing in large sources of new power generation which might sit idle for long periods of time. Accordingly, they developed an interest in what came to be known as Advanced Metering Infrastructure (AMI), which can be used to implement hourly billing plans that incentivize consumers to shift electricity use from times of high demand to times of low demand. Microprocessors could also be used to help integrate Distributed Energy Resources (DER) such as rooftop solar, wind, and demand response programs, wherein customers might agree to stop using energy at certain times in exchange for more favorable rates.[12]

12. Rebecca Slayton, *Efficient, Secure Green: Digital Utopianism and the Challenge of Making the Grid "Smart*," 48 INFO. & CULTURE 448, 455–57 (2013).

In the 1990s, advocates of market restructuring also argued that computer networking could enable the creation of more competitive spot markets, or markets where financial instruments are traded for immediate delivery of services or goods. At the time, electricity production followed a model in which vertically integrated utilities provided electricity generation, transmission, and distribution as regulated monopolies. Spot markets would have utilities primarily provide transmission and distribution as regulated monopolies, while companies competed to supply generation. The 1992 Energy Policy Act authorized the Federal Energy Regulatory Commission (FERC) to require that utilities make their transmission lines available to electricity generators that wanted to sell wholesale power to distributors. FERC acted aggressively on its new authority, and some state commissions went further by requiring utilities to divest their generation assets.[13]

FERC encouraged utilities to form non-profit Independent System Operators (ISOs) or Regional Transmission Operators (RTOs) to manage centralized spot markets and coordinate grid operations.[14] Here again, information technology (IT) played a key role in the new regime. The ISOs/RTOs used computer networks (including the internet) to create a centralized spot market on a day-ahead and hourly basis. Electricity generators bid to supply electricity at specific times, and the ISOs/RTOs used these bids to manage economic dispatch for the system.[15] Today, approximately two-thirds of the electricity supply in North America is coordinated by nine different ISO/RTOs.[16]

Thus, the rise of distributed energy resources, along with the creation of spot markets and associated unbundling of generation and distribution, entailed a transformation in the information infrastructure running the electrical grid in the final decades of the twentieth century. The infrastructure transformed from a system controlled primarily by special-purpose and centralized computers towards one controlled by a complex network of standardized and distributed microprocessors.

---

13. *See* THE ELECTRIC ENERGY MARKET COMPETITION TASK FORCE, REPORT TO CONGRESS ON COMPETITION IN WHOLESALE AND RETAIL MARKETS FOR ELECTRIC ENERGY, 33–34 (2006).

14. Promoting Wholesale Competition Through Open Access Non-discriminatory Transmission Services by Public Utilities; Recovery of Stranded Costs by Public Utilities and Transmitting Utilities, 61 Fed. Reg. 21540, 21596–97, (May. 10, 1996) (codified at 18 C.F.R. pts. 35, 385) (encouraging the formation of ISOs).

15. Seth A. Blumsack, Jay Apt & Lester B. Lave, *Lessons from the Failure of U.S. Electricity Restructuring*, 19 ELECTRICITY J. 15, 17–19, 26 (Mar. 2006).

16. ISO/RTO COUNCIL, https://isorto.org (last visited Feb. 24, 2020).

Around the turn of the millennium, this transformation was accelerated by growing enthusiasm for a smart grid—a label incorporating a vast range of technologies such as advanced metering infrastructure, electric vehicle charging stations that can also provide battery storage and related services, satellite-based, wide-area measurement systems, and many more computer-managed systems.[17] The U.S. Energy Independence and Security Act of 2007 committed the nation to developing a smart grid, defined first and foremost as the "increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid," followed by the "[d]ynamic optimization of grid operations and resources, with full cybersecurity," the "[d]eployment and integration of distributed resources and generation, including renewable resources," and a list of other goals.[18] In sum, the smart grid is typically depicted as something that will simultaneously increase efficiency, reliability, security, and the integration of renewable resources.

However, there are tradeoffs between these goals in practice.[19] While some smart devices may improve security, the proliferation of "smart" devices—particularly through the distribution systems that local and state regulators oversee—also greatly increases opportunities for attack. Accordingly, the 2007 Act also gave the National Institute of Standards (NIST) responsibility for coordinating the development of a framework to ensure the interoperability and security of these many devices. NIST published this framework in August 2010, including a set of high-level cybersecurity guidelines.[20] However, these were not mandatory requirements, and they left considerable room for discretion to experts in the industry to determine what constituted appropriate risk. As the framework explained, "[e]ach organization will need to perform a risk assessment to determine the applicability of the requirements to their specific situations."[21]

The NIST guidelines were partly based on federal cybersecurity standards, which were mandatory for the bulk electric grid—i.e., generation and transmission assets. Yet, as the following sections discuss, these federal standards were also risk-based and left considerable room for experts to exercise discretion.

17. *See* Slayton, *supra* note 12, at 464–65.

18. Energy Independence and Security Act of 2007 § 1301, 42 U.S.C. § 17381 (2018).

19. Slayton, *supra* note 12, at 460–68.

20. *See* CYBER SEC. WORKING GRP., NAT'L INST. OF STANDARDS & TECH., INTRODUCTION TO NISTIR 7628: GUIDELINES FOR SMART GRID CYBER SECURITY 2 (2010) https://permanent.access.gpo.gov/gpo1900/nistir-7628_total.pdf.

21. *Id.* at 10.

B. THE INDETERMINACY OF FEDERAL CYBERSECURITY REGULATIONS[22]

Though engineers began to warn of computer-related security risks as early as the 1970s, regulators paid relatively little attention to what came to be known as cybersecurity until the late 1990s. The Oklahoma City bombings focused federal attention on critical infrastructure protection, which only intensified after the 2001 terrorist attacks on the World Trade Center. FERC announced that it would be including cybersecurity standards in its 2002 Notice of Proposed Rulemaking on a Standardized Market Design, which was intended to provide a "level playing field" for competitive wholesale electric markets.[23] It asked an industry group—the North American Electric Reliability Corporation (NERC)—to help draft standards. Over the next year, NERC helped to manage an often-controversial standards drafting process. On August 13, 2003, it approved an "Urgent Action Standard" intended to serve as a temporary guide until more permanent standards could be agreed upon.[24]

The very next day, the largest blackout in U.S. history left fifty-five million people without power across eight U.S. states and Ontario, Canada. A task force charged with examining the causes of the blackout implicated software: a glitch caused an alarm malfunction after a transmission line hit a tree branch, leading to a cascading failure with widespread consequences.[25] The task force's final report further noted that "there are terrorists and other malicious actors who have the capability to conduct a malicious cyberattack with potential to disrupt the energy infrastructure."[26] Consequently, it recommended including physical and cybersecurity requirements in a set of reliability standards which were to be "mandatory and enforceable, with penalties for noncompliance."[27]

The Energy Policy Act of 2005 began implementing these recommendations by tasking FERC with designating an electric reliability organization (ERO), which would work with the industry to develop and enforce the new standards. NERC was the only entity to file for ERO consideration and was appointed as ERO in July 2006.[28]

However, the process of developing enforceable Critical Infrastructure Protection (CIP) standards was slow, partly because of significant tensions between the expert practices needed for maintaining the reliability of the grid's

22. Much of the discussion in this Section is based on research presented in Slayton & Clark-Ginsberg, *supra* note 8. More detailed discussion and citations can be found there.

23. *Id.* at 120.

24. *Id.* at 121.

25. U.S.-CAN. POWER SYS. TASK FORCE, *supra* note 3, at 135.

26. *Id.*

27. *Id.* at 163.

28. Energy Policy Act of 2005 § 1211, 16 U.S.C. § 824o (2018).

operational technology (OT)—physical machinery such as electricity generators, circuit breakers, transformers—and those that have traditionally been used for securing IT. OT engineers have achieved tremendous levels of reliability through a slow and evolutionary process of change, deploying technology for decades at a time. By contrast, IT is secured through frequent software updates, and systems are often outdated within five years.[29] Software updates can often produce unexpected consequences and interactions. While such unexpected behavior is an inconvenience in an office environment, it can be deadly when the computers control physical machinery. The companies making control systems for OT have not always provided software patches and may not support capabilities such as encryption. Password protection and other common forms of authentication may be dangerous if they lock out an operator in an emergency. Thus, OT and IT have struggled to agree upon what the CIP standards should entail or what constitutes best practices in critical infrastructure cybersecurity.

These tensions led to exceptions within the NERC CIP standards which allowed organizations to use "reasonable business judgment" in determining whether or not to apply security controls[30] Utilities were particularly concerned about the potentially prohibitive cost of replacing equipment that had been expected to last for decades, simply because that equipment did not allow for the implementation of certain controls. However, exceptions based upon "technical feasibility" and "business judgment" gave industry experts more discretion than regulators wanted.[31] When FERC approved the standard in January 2008, it also required NERC to remove "language that allowed variable implementation of standards based on 'reasonable business judgment' " and to create "a new framework of accountability surrounding exceptions based on technical feasibility."[32] Nonetheless, federal regulators continue to be challenged by the inevitable need for industry experts to use some discretion in implementing standards, as well as the need to adjudicate when experts do not agree.

---

29. JOSEPH WEISS, PROTECTING INDUSTRIAL CONTROL SYSTEMS FROM ELECTRONIC THREATS 34 (2010).

30. *FERC Approves New Reliability Standards for Cyber Security*, POWERGRID INT'L, Jan. 17, 2008, https://www.power-grid.com/2008/01/17/ferc-approves-new-reliability-standards-for-cyber-security/#gref; *see also*, Mandatory Reliability Standards for Critical Infrastructure Protection, 17 Fed. Reg. 7368, 7370 (Feb. 7, 2008) (codified at 18 C.F.R. pt. 40).

31. *Id.*

32. *See* Mandatory Reliability Standards for Critical Infrastructure Protection, *supra* note 30, at 7370; POWERGRID INT'L, *supra* note 30. Under the approved standards, organizations would be required to self-certify compliance more than once a year, and to "achieve 'auditable compliance' no earlier than mid-2009." Mandatory Reliability Standards for Critical Infrastructure Protection, 17 Fed. Reg., *supra* note 30, at 7371.

State and local authorities face these challenges to an even greater degree. For example, public utility commissions must regularly assess whether utilities' requests for rate recovery related to NERC CIP compliance requirements is justified. Furthermore, NERC CIP standards were designed to protect electricity generation and transmission infrastructure, not the distribution networks that fall under the jurisdiction of state and local authorities. Indeed, the reliability and security of distribution networks are regulated through a patchwork of state and local organizations. Investor-owned utilities are regulated by state utility commissions, while municipal utilities are owned by cities and are held accountable by elected officials, and cooperatives are owned and governed by their members.

Decision-makers in this patchwork of governing bodies may have little or no knowledge of cybersecurity. Nor do they always have the resources needed for assessing tradeoffs between security and other public goods. Yet they are responsible for overseeing some of the most vulnerable and exposed portions of the electric power grid. The remainder of this Article examines how one such organization—the New York Public Services Commission (NYPSC)—has responded to this challenge. It then briefly compares that to the response of another organization—the Massachusetts Department of Public Utilities.

C. ORGANIZING EXPERTISE AT THE NEW YORK PUBLIC SERVICE COMMISSION

The NYPSC is a particularly interesting case because the terrorist attacks of September 11, 2001, put the Commission literally at ground zero of debate about critical infrastructure security. One month after the terrorist attacks on the Twin Towers, the Commission established a security assessment team within its staff arm, the Department of Public Service.[33] This team began meeting with the dozens of companies within its jurisdiction to develop a better understanding of the security measures in place.[34] In 2003, the Commission hired John Sennett, who had been a special agent with the FBI since 1980, to direct a new utility security section.[35] Over the next several years, the security section hired individuals specializing in physical security—many of whom had a background in law enforcement—as well as individuals with training in information security.

33. Lori A. Burkhart, *A Fight Over Market Design*, PUB. UTIL. FORTNIGHTLY (Nov. 15, 2002), https://www.fortnightly.com/fortnightly/2002/11-0/regulators-forum-fight-over-market-design.

34. *Id.*

35. Neither Sennett nor the security section has a public profile associated with the commission, but Sennett's background appears on his professional website. *See* John Sennett, LINKEDIN, https://www.linkedin.com/in/john-sennett-25a16529 (last visited Aug. 1, 2020).

However, the Department did not wait until it had hired in-house security experts to begin evaluating the utilities' security. Instead, staff immediately urged the energy and telecommunications utilities to "retain third-party consultants or experts to evaluate the adequacy of their physical equipment and computer system security arrangements."[36] Most of the companies did so, but two of the twelve—New York State Electric & Gas (NYSEG) and MCI Communications Corporation (originally Microwave Communications Inc.)—balked. Accordingly, in August 2002, the Commission ordered the NYSEG and MCI to retain consultants to evaluate their security. Additionally, noting that the Commission staff and utilities "have not faced a threat of this magnitude and scope in the past," the Commission argued that "outside expertise is needed to ensure that preparations to meet the new threats are adequate."[37] Accordingly, the Commission contracted with two consulting firms—one firm to evaluate the adequacy of the cybersecurity evaluations and the utilities' response to recommendations in those evaluations, and another firm to do the same with the physical security evaluations.

The two firms ultimately found that, while the utilities were diligent about contracting for third-party security assessments, those assessments sometimes overlooked issues such as the need for separation of duties and policies for managing personnel and third-party vendors. In September 2003, the Commission ordered the utilities to prepare management plans explaining how they would respond to the issues raised in the reports that the utilities had contracted, in addition to those contracted by the Commission.[38]

In June 2004, it issued a press release announcing that the energy utilities had implemented or were in the process of implementing "a total of almost 800 initiatives designed to strengthen physical and cyber-system security," while telecommunications companies were implementing 275 such initiatives.[39] Furthermore, it explained:

---

36. Order Instituting Proceeding and Establishing Procedures for Preparation of Security Evaluations at 1, Telephone and Energy Utility Arrangements for Safeguarding the Security of Their Physical Equipment and Cyber Systems, No. 02-M-0953 (N.Y. Pub. Serv. Comm'n Aug. 2, 2002), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={C2E5B25F-CDFB-42DB-A405-6647EDD6AD33}.

37. *Id.* at 2.

38. *See generally* Order Directing Further Action, Telephone and Energy Utility Arrangements for Safeguarding the Security of Their Physical Equipment and Cyber Systems, No. 02-M-0953 (N.Y. Pub. Serv. Comm'n Sep. 30, 2003), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={4E6EC1D8-227D-4C6B-A741-D2D668DEACB4}.

39. Press Release, N.Y. Pub. Serv. Comm'n, Strengthening of Physical and Cyber-System Security of Energy/Telecommunications Utilities Protects Public (June 2, 2004), http://

> The Commission's Office of Utility Security staff has conducted its own analysis of the utility efforts, with assistance from selected independent security experts, and determined that physical and cyber-system security involving utility facilities in the state is greatly improved. Moreover, Commission staff, in concert with the utilities, will continue to evaluate emerging technologies for continually improving security.[40]

As these words suggest, the Commission's security experts aimed to accomplish their work in a collaborative rather than an adversarial manner, working "in concert" with the utilities.[41] Below, I will argue that this collaborative approach was sometimes conducive to achieving a persuasive public performance of expertise because ambiguities about how to apply standards could be resolved behind closed doors, rather than in a public forum where the contingent and value-laden nature of expert judgments can be questioned. Nonetheless, experts' ability to perform persuasively has varied across different contexts. The following parts discuss three such contexts: responding to security breaches at the utilities, evaluating requests for rate recovery of cybersecurity expenses, and establishing standards for an increasingly complex and divided industry.

III. EXPERTISE IN THE BREACH

Despite the Commission's efforts to bolster both physical and cybersecurity at its regulated utilities in the early 2000s, these organizations were not free of breaches over the following decade. The most significant known breach was discovered in January 2012, after IT staff at NYSEG and Rochester Gas & Electric (RG&E) noticed suspicious network traffic that used the access credentials of one of the companies' contractors. They soon concluded that the confidential information of approximately 1.8 million customers—including social security numbers, birthdates, and financial account information—had been compromised. They consequently issued notifications to customers, along with offers of credit monitoring services.[42] The companies retained Verizon Business to conduct an investigation, which

www3.dps.ny.gov/pscweb/WebFileRoom.nsf/Web/1D5D816E2F80B95D8525729D00655 96C/$File/pr04042.pdf?OpenElement.

40. *Id.*

41. *Id.*

42. *See* Staff Report at 4, Order Directing a Report on the Implementation of Recommendations, N.Y. State Elec. & Gas Corp./Rochester Gas & Elec. Corp. Sec. Breach, No. 12-M-0282 (N.Y. Pub. Serv. Comm'n July 18 2012), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={94D18677-4E68-4549-88FD-6FCB29703A03}.

discovered that the contractors had subcontracted work to persons working outside of the United States. It found no wrongful intent on the part of the contractor or the subcontractor and no evidence that any of the information had been used. Nonetheless, the Commission ordered its security staff to investigate the cybersecurity practices of NYSEG, RG&E, and other regulated utilities.[43]

In July, the security specialists issued a report identifying five areas in which NYSEG and RG&E had failed to follow "best practices" as defined in NIST standards for protecting personally identifiable information.[44] They also noted that they had completed on-site reviews of four companies—Consolidated Edison, Orange and Rockland, National Grid, and National Fuel Gas—and would soon complete a comparable review of Central Hudson.[45] They had not discovered any "significant vulnerabilities requiring immediate corrective action," but they had identified some "areas for improvement," and they expected the utilities to implement their recommendations.[46] In September, the staff sent out a questionnaire to all the utilities for an on-site review by the Commission staff, which would be scheduled no later than October 31, 2012.[47]

If the Commission staff found major problems at Central Hudson, it did not mention them in any public documents. Yet on February 16, 2013, IT staff at Central Hudson found evidence of anomalous activity on their networks.[48] Over the next three days, they discovered an active worm in their system.[49] Moreover, a computer connected to a cash and check processing system was trying to log on to other company computers using local accounts.[50] The staff notified the utility security section of the Department of Public Services and

43. *See* Press Release, N.Y. Pub. Serv. Comm'n, PSC Investigates Consumer Data Breach at NYSEG, RG&E (Jan. 23, 2012), http://www3.dps.ny.gov/pscweb/WebFileRoom.nsf/Web/1986D5ECA1917A8A8525798E005F81DD/$File/pr12007.pdf?OpenElement.

44. The staff's report is appended to the Commission's order issued six days later. *See* Staff Report, *supra* note 42, at 3.

45. *Id.* at 13.

46. *Id.* at 14.

47. *See* Letter from Jaclyn A. Brilling, N.Y. State Elec. & Gas Corp./Rochester Gas & Elec. Corp. Sec. Breach, No. 12-M-0282 (N.Y. Pub. Serv. Comm'n Sep. 20, 2012), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={09628D61-47C9-43D6-97D5-3606771E6170}.

48. Order Directing the Creation of an Implementation Plan at 1, Security for the Protection of Personally Identifiable Customer Information, No. 13-M-0178 (N.Y. Pub. Serv. Comm'n Aug. 19, 2013) (rev. of Cent. Hudson Gas & Elec. Corp. Breach Incident), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={28CDF9EB-8661-491C-B2C2-E6E527297EE0}.

49. *Id.* at 1–2.

50. *Id.* at 1.

contracted with Dell to investigate further.[51] Experts from Dell concluded that the malware had been present for at least six months prior to discovery but could not determine how it had been introduced or how much data it might have extracted from the system.[52] Central Hudson had no choice but to regard the checking information of its customers as compromised, and on February 22, 2013, it began to notify the public and approximately 110,000 affected customers.[53] Dell ultimately made thirteen recommendations to Central Hudson.[54]

The Commission's security staff met with Central Hudson and Dell's representatives and reported on the process to the Commission, which ordered Central Hudson to file an implementation plan outlining how it would respond to the issues raised by Dell. Meanwhile, the Commission's security experts continued to review the utilities and ultimately made nine recommendations for improving security, including several "best practices"—preparing for breaches by conducting drills and contracting with forensic experts and credit monitoring companies, improving training, improving management of personally identifiable information, upgrading both physical and cyber defensive measures such as "next-generation intrusion detection systems," and conducting a regular third-party vulnerability assessment.[55]

In August 2013, the Commission ordered each of the utilities to prepare plans outlining how they were implementing these recommendations.[56] Furthermore, arguing that the final measure—regular vulnerability assessments—was the most important of the nine recommendations, the Commission ordered each utility to undertake an annual vulnerability assessment, the first of which was to be completed by July 1, 2014.[57] The Commission emphasized that it was important "that any third-party consultants retained for this purpose have a high level of experience and expertise," and noted that its staff had recommended "certification by the Payment Card Industry Security Standards Council" as "the best available

51. *Id.* at 2.
52. *Id.* at 2–3.
53. *Id.* at 3.
54. *Id.* at 6.
55. Order Directing the Creation of an Implementation Plan at 5–6, Security for the Protection of Personally Identifiable Customer Information, No. 13-M-0178 (N.Y. Pub. Serv. Comm'n Aug. 19, 2013), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={5986D197-87DB-4D21-A89B-95DC45E05061}.
56. *See, e.g.*, *id.* at 8.
57. *Id.* at 7.

assurance of competence for this type of audit work."[58] The Commission's security staff would then review the implementation plans.

In sum, the breaches at NYSEG and Central Hudson led the Commission to establish new oversight practices, most notably an annual third-party audit. Since no major breaches have come to light since the Commission instituted annual audits and investigations never found evidence of data misuse, the incidents appear to have been publicly resolved. Nonetheless, perhaps it is remarkable that the breaches were never used to question the expertise of either the utilities' or the Commission's security staff. After all, why was it that even after specifically investigating security practices at the utilities, the Commission's staff did not publicly identify and correct the shortcomings that led to the breach at Central Hudson? But this question does not appear to have been asked publicly. Instead, the breach provided an opportunity for the Commission's experts to perform expertise by citing best practices, certifications, and other institutionalized markers of cybersecurity expertise. Rather than demonstrating a lack of expertise among these professionals, the Commission took these incidents as proof that their expertise was needed.

IV. RATE RECOVERY AMID PERPETUALLY EVOLVING THREATS

A second context in which the Commission's staff have performed expertise is in the evaluation of requests to recover expenses associated with cybersecurity. In this context, we must note a significant tension between two needs—the need for continual investment in cybersecurity to counter continually evolving threats and the need to keep rates affordable and stable over time.

In the past decade, utilities have repeatedly rationalized requests to recover expenses associated with cybersecurity by highlighting new and changing threats to the grid. Most of these requests have been buried in much larger and more comprehensive rate cases, some of which proved quite controversial, with some of the Commission's in-house experts challenging proposed utility expenditures. Nonetheless, the Commission's cybersecurity staff have generally embraced arguments for increased spending on security, citing rapidly changing threats.

For example, in June 2013, six months after initiating a comprehensive rate case, Con Edison increased its request for cybersecurity investment. In prepared testimony, Con Edison's in-house experts argued that "cyber threats are becoming more persistent, more sophisticated, more widespread, with a

58. *Id.* at 7–8.

greater focus on the utility industry and with potentially severe consequences . . . ."[59] They highlighted recent attacks on utilities, including the compromise of the control systems of a northeast utility, and an ongoing targeted attack on Con Edison's internal computer networks from internet addresses in Iran. While emphasizing that they did not believe the attack on Con Edison had been successful, they noted that "[t]here is no reason to assume these attacks will abate . . . [i]n fact, all recent evidence indicates they will continue to occur with increasing sophistication and as attack vectors change, the Company's responses to them must be swift and definitive."[60] Accordingly, they requested rate recovery for capital investments as well as operational and maintenance expenses associated with the hiring of sixteen new cybersecurity experts. Many aspects of Con Edison's rate case proved contentious, with the Commission staff rejecting portions of Con Edison's requested revenue increases. However, the Commission's security staff did not oppose these new investments in cybersecurity.[61]

Three years later, when Con Edison again requested new revenues associated with cybersecurity, the Commission's security staff not only accepted that such expenses were necessary, they also repeated the rationale of evolving threats in their prepared testimony. Their rationale was that:

> [t]he field of cybersecurity is one in which the risks, threat actors/vectors, and technologies involved are constantly changing and increasing in complexity at a breakneck pace. . . . This ever-escalating cyber threat to business and critical infrastructure information requires that utilities remain constantly vigilant and seek new and innovative ways to bolster their cybersecurity posture.[62]

Both utility and Commission cybersecurity experts repeated similar arguments in a recent rate case filed by NYSEG and RG&E. In May 2019, testimony from the company's electric reliability and operations panel argued that

59. Prepared Testimony of the Shared Services Panel at 14, In the Matter of Consolidated Edison Co. of N.Y., Inc., Nos. 13-E-0030, 13-G-0031, 13-S-0032 (N.Y. Pub. Serv. Comm'n June 21, 2013), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={C69D0A46-1A04-461A-A25D-6B5BD131984F}.

60. *Id.* at 14.

61. *See* Staff Initial Brief, In the Matter of Consolidated Edison Co. of N.Y., Inc., Nos. 13-E-0030, 13-G-0031, 13-S-0032 (N.Y. Pub. Serv. Comm'n Aug. 30, 2013), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={BBA1148B-18D6-4A85-BEAD-B6C6FB042E37}.

62. Keith Haugen & Dennis C. Murray, Prepared Testimony of the Department of Public Service Staff Security Panel at 19, In the Matter of Consolidated Edison Company of New York, Inc., Nos. 16-E-0060, 16-G-0061 (N.Y. Pub. Serv. Comm'n 2016), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={DBE70276-BD3C-46F6-80E9-A8B878BC3D8A}.

"continual and extensive changes to the security landscape require these security upgrades to protect against physical and cyber intrusions. . . . As threats evolve and become more sophisticated, the Companies must keep pace."[63] It also noted that growing cybersecurity expenses were needed "to ensure data protection, privacy and compliance with regulatory and legal mandates."[64]

The Commission's cybersecurity experts echoed these arguments in prepared testimony.[65] When asked to explain the importance of cybersecurity, they argued that "[t]he field of cyber security is one in which the risks, threat actors/vectors, and technologies involved are constantly changing and increasing in complexity."[66] They used similar rhetoric to recommend approval of proposals for increased spending for a previously funded project, the "Net Sec[urity] Lifecycle," noting that "the projects that comprise the multiple layers of security need to be constantly maintained and upgraded, and both software and hardware need periodic replacement."[67]

To be sure, staff evaluating these proposals cited more than just evolving threats. They also pointed to NERC's mandatory cybersecurity standards, along with other best practices. Yet as discussed above, existing standards of grid security leave considerable room for discretion. Perhaps remarkably, I have yet to find any examples of the New York Public Service Commission security staff critiquing the utilities' grid cybersecurity proposals. This suggests that they are either spending too much on cybersecurity or failing to adequately secure the grid. This substantial agreement between the utilities' and Commission's experts may largely be due to a tacit and informal coordinating process that takes place as the Commission staff conduct their regular oversight work.

---

63. Direct Testimony of Electric Reliability & Operations Panel at 33–34, No. 19-E-0378 (N.Y. Pub. Serv. Comm'n May 20, 2019), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={21DC1333-30C6-4989-9C76-E2617E2D96EC}.

64. *See id.* at 34.

65. Specifically, testimony was provided by Brian O'Keefe, who held a BS in political science and extensive experience in managing physical security at National Grid, and Philip Tabor, a cybersecurity analyst who held a BS in psychology and a Security+ certification from the Computing Technology Industry Association (Comp TIA), a certifying body. Keith Haugen Dennis C. Murray, Prepared Testimony of the Department of Public Service Staff Security Panel, before the State of New York Public Service Commission, In the Matter of Consolidated Edison Company of New York, Inc. Cases 16-E-0060 and 16-G-0061 (2016)

66. Prepared Testimony of Staff Security Panel at 15, Office of Resilience and Emergency Preparedness, No. 19-E-0378, 19-G-0379, 19-E-0380, 19-G-0381 (N.Y. Pub. Serv. Comm'n Sept. 20, 2019), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={BF742238-7AF2-478D-A6E1-88C58477EF76.

67. *Id.* at 17.

A. REJECTING THE RHETORIC OF CONTINUALLY EVOLVING THREATS

In states where public utility commissions have devised other means to gather expert advice, the same kinds of arguments for increased investment in cybersecurity have not always proven persuasive. This becomes very clear from a recent case in Massachusetts. Unlike the New York Public Services Commission, the Massachusetts Department of Public Utilities does not appear to have an in-house team of security experts. Instead, the Massachusetts Attorney General's Office (AGO) has a section devoted to ratepayer advocacy. This section represents the ratepayers in any proceeding and can hire consultants and charge back the costs to the companies.[68] The AGO recently played a significant role in challenging proposals for rate recovery related to IT, including cybersecurity.

In 2019, Massachusetts Electric Company and Nantucket Electric Company, two subsidiaries of the multinational National Grid Services Company, filed a comprehensive rate case with the Massachusetts Department of Public Utilities. One of seventeen sets of testimony submitted by National Grid focused on IT.[69] The Information Technology Panel explained that the company's Digital Risk and Security team provided "the requisite consultancy and expertise needed to meet the escalating threats to the Company's networks and systems."[70] It further explained that it had recently "revisited its strategy and associated project roadmaps to ensure that the roadmaps were in alignment with the current threat landscape," and that this review "resulted in a refreshed multi-year investment program needed to ensure continued and evolving protection of National Grid's cyber and information assets."[71] The panel outlined eight new initiatives in an attached exhibit, arguing that these would "deliver new capabilities focused on ensuring the reliability and availability of our infrastructure, while delivering capability to keep pace with

68. MASS. GEN. LAWS ch. 12, § 11E (2020).

69. The panel included three employees: Stephen Olive, Chief Information Officer, who holds a bachelor's degree in electrical engineering and an MBA; Daniel J. DeMauro, NGSC's director of U.S. information technology regulatory compliance, who holds a bachelor's degree in accounting; and Mukund Ravipaty, NGSC's Director of Global Head Security Services, Design, and Architecture, who holds a bachelor's degree in computer science and an MBA. Ravipaty described his responsibilities as including "overseeing the development of cyber-security strategy and architecture to ensure that National Grid's cyber and security protections are developed to keep pace with the evolving threats and capabilities of hostile individuals, groups, and nations." Pre-Filed Direct Testimony of the Information Technology Panel at 184, Mass. Elec. Co. & Nantucket Elec. Co. each d/b/a Nat'l Grid, D.P.U. 18-150 (Mass. Dep't of Pub. Util. Nov. 15, 2018), https://fileservice.eea.comacloud.net/FileService.Api/file/FileRoom/10043017.

70. *Id.* at 192.

71. *Id.* at 194.

emerging threats and continued evolution towards a risk based, proactive, intelligence led cyber security program."[72]

In November 2018, the AGO responded to the National Grid filing by requesting approval to spend up to $550,000 on consultants, citing the high complexity of the case and a substantial rate increase.[73] This request was quickly granted, and both the AGO and Department of Public Utilities were soon issuing dozens of information requests to National Grid. This included queries about proposed cybersecurity programs, including "whether each project or investment enhances current IT assets/capabilities, or replaces existing IT assets/capabilities" and "if the existing assets have reached the end of their useful life and how the Company has adjusted its associated cost accounting."[74]

National Grid's expert panel responded that all the proposed investments "are either new or enhanced capabilities."[75] It further explained: "[d]ue to the nature and sophistication of the continuing cyber threats, National Grid is continually developing its cyber capabilities to stay one step ahead of these emerging threats."[76] National Grid also attached a February 2019 IT strategy document, prepared by a consultant to the company, which emphasized the need for continual change:

> In today's global ecosystem, the threat of cyber-attacks has continued to intensify and grow in complexity. This ever-changing landscape requires continued focus and attention to safeguard the critical national infrastructure . . . .
>
> National Grid must continue to develop its cyber capability, at a faster pace than the emerging threats, and this is becoming

72. *Id.*

73. The Attorney General's Notice of Retention of Experts and Consultants, Mass. Elec. Co. & Nantucket Elec. Co. each d/b/a Nat'l Grid, D.P.U. 18-150 (Mass. Dep't of Pub. Util. Nov. 27, 2018), https://fileservice.eea.comacloud.net/FileService.Api/file/FileRoom/10071059.

74. Attorney General's Thirtieth Set of Document and Information Requests at 1, Mass. Elec. Co. & Nantucket Elec. Co. each d/b/a Nat'l Grid, D.P.U. 18-150 (Mass. Dep't of Pub. Util. Mar. 15, 2019), https://fileservice.eea.comacloud.net/FileService.Api/file/FileRoom/10479171.

75. Information Request AG-30-1 at 2, Mass. Elec. Co. & Nantucket Elec. Co. each d/b/a Nat'l Grid, D.P.U. 18-150 (Mass. Dep't of Pub. Util. Mar. 29, 2019), https://fileservice.eea.comacloud.net/FileService.Api/file/FileRoom/10546443.

76. *Id.* at 2.

> increasingly critical as the energy sector evolves and accelerates the digitisation of energy infrastructure . . . .[77]

National Grid also responded to a range of other information requests, such as which projects would address compliance with NERC CIP requirements, and what costs were allocated to National Grid's subsidiaries operating in different regions. As we have seen, similar arguments about the need to keep pace with growing threats satisfied the New York Public Service Commission when faced with such a request.

However, the Massachusetts Attorney General deemed these responses deficient. In a brief filed in mid-June 2019, the AGO criticized National Grid's "high level description of projects," continuing:

> The Company's investment "plan" constitutes an accumulation of disjointed documents without a comprehensive planning document to pull them all together. The Company's documents show an investment process that is subject to continual adjustments, unstructured relative to long-term initiatives and spending…and contains no performance measurements or benchmarks. . . . [T]he Company's approach of producing an annual portfolio of projects subject to continual change is unacceptable given the significant and increasing level of IT investment.[78]

For its part, National Grid argued that criticism about continual change was inappropriate since changes were responsive to real needs and were thoroughly reviewed.

In its final order, the Massachusetts Department of Public Utilities ultimately concluded that National Grid's proposed costs associated with IT investments were "reasonable" and actually slightly increased the proposed IT rent expense.[79] Nonetheless, it found "some merit in the Attorney General's argument that the Company's approach to IT investment is reactive, uncoordinated, and has not been vetted to determine benefits Massachusetts ratepayers receive for the costs allocated to them."[80] This was just one of several concerns that spurred the Massachusetts Department of Public Utilities

77. Attachment AG-30-1-2 at 8, Mass. Elec. Co. & Nantucket Elec. Co. each d/b/a Nat'l Grid, D.P.U. 18-150 (Mass. Dep't of Pub. Util. Mar. 29 2019), https://fileservice.eea.comacloud.net/FileService.Api/file/FileRoom/10546446.

78. Initial Brief of the Office of the Attorney General at 48, Mass. Elec. Co. & Nantucket Elec. Co. each d/b/a Nat'l Grid, D.P.U. 18-150 (Mass. Dep't of Pub. Util. June 14, 2019), https://fileservice.eea.comacloud.net/FileService.Api/file/FileRoom/10831974.

79. Order at 71, 269, 271 Mass. Elec. Co. & Nantucket Elec. Co. each d/b/a Nat'l Grid, D.P.U. 18-150 (Mass. Dep't of Pub. Util. Sept. 30, 2019), https://fileservice.eea.comacloud.net/FileService.Api/file/FileRoom/11262053.

80. *Id.* at 499.

to open an investigation into the company's strategic planning processes, staffing decisions, and "potential management problems through to the highest levels of the organization."[81]

As this suggests, arguments that rapidly evolving threats necessitate increased cybersecurity funding are not always persuasive to government authorities charged with protecting ratepayer interests. The outcomes of the cases cited here are underdetermined by the arguments of experts and likely reflect the different processes by which experts mediate between the utilities and regulators. In sum, the AGO hiring of consultants to scrutinize the utilities' proposals as needed is an intrinsically more adversarial process, whereas the New York Public Service Commission's in-house cybersecurity experts are likely to develop cooperative relationships with the utilities' experts.

V. CYBERSECURITY STANDARDS FOR A RAPIDLY EVOLVING INDUSTRY

A third context in which the New York Department of Public Services security section has performed expertise is in helping to establish standards for a rapidly changing industry. As noted above, efforts to achieve a variety of regulatory goals—including the increased integration of renewable resources and the introduction of more retail competition and lower energy prices—have driven investments in IT that inevitably create new security vulnerabilities. The New York Public Service Commission was proactive about industry restructuring and began pushing retail competition in energy supply in the 1990s. In the restructured market, Energy Service Companies (ESCOs) began competing to purchase and sell energy resources, such as demand-side response capabilities (programs which incentivized users to not use energy at times of high demand), tailoring the specific mix to the needs or interests of particular customers.[82] ESCOs were seen as important to achieving goals for integrating more renewable energy into the grid because they could, for example, give consumers the option to pay more for energy from renewable resources. Utilities became providers of infrastructure, but no longer held monopoly power to sell electricity.

81. *Id.* at 502.

82. ESCOs also may offer many other services, such as helping large energy consumers reduce their consumption. But for purposes of this discussion, I am focusing on their role in competitive energy markets. For an early discussion of the role of ESCOs in restructured markets, see Opinion and Order Concerning Uniform Business Practices, Retail Access Business Rules, No. 98-M-1343 (N.Y. Pub. Serv. Comm'n Feb. 16, 1999), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={8543A612-83DD-45E3-9262-EB1CBF591743}.

Enabling this restructured market entailed the creation of an Electronic Data Interchange (EDI) that the utilities, ESCOs, direct customers, and marketers could use to exchange data. In the late 1990s, the Commission started an EDI working group to establish standards.[83] Creating market incentives and signals also entailed the deployment of Advanced Metering Infrastructure to enable time-of-use billing. In 2006, the Commission ordered utilities to file plans for deploying AMI.[84] As the utilities began submitting their plans, the Commission concluded that the utilities did not share a common understanding of what features AMI should include. Accordingly, on October 10, 2007, the Commission requested comment on what minimum functional requirements should be included in AMI.[85] And in April 2008, the Commission held a technical conference on the topic.[86]

It was only at this technical conference that the Commission staff finally began to devote significant attention to the security of AMI. They formed a "utility AMI security task force" which began to work "intensively."[87] However, by February 13, 2009, when the Commission issued minimum technical requirements, the task force reported that it had "much work yet to do before producing technical specifications that may be used by utilities to assess and procure security related functionality."[88] It noted "[s]ecurity must be built in from the beginning to be truly effective, but often it is the lowest consideration as all of the other competing demands are being pursued."[89] While acknowledging that they had "only begun to scratch the surface of addressing security issues" and that requirements would need to be revisited, they articulated nine security capabilities that they reviewed as necessary; these included authenticating users, maintaining data integrity and confidentiality, and providing audit logs and administration tools.[90]

---

83. *Id.* at 9–10.

84. *See* Notice Seeking Comment at 1, Competitive Metering, No. 00-E-0165 (N.Y. Pub. Serv. Comm'n Oct. 10, 2007), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={F81FB762-3011-4AB9-949B-EF73D78B88C1}.

85. *See id.* at 1–2.

86. *See* Notice of Technical Conference on Advanced Metering Infrastructure, Competitive Metering, No. 00-E-0165 (N.Y. Pub. Serv. Comm'n Mar. 3, 2008), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={4DC3DCBF-0974-44FC-BA74-003E9D1FCDFE}.

87. Order Adopting Minimum Functional Requirements for Advanced Metering Infrastructure Systems and Initiating an Inquiry into Benefit-Cost Methodologies at 16, Advanced Metering Infrastructure, No. 09-M-0074 (N.Y. Pub. Serv. Comm'n Feb. 13, 2009), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={16310751-0A41-401D-BFE5-7E95F5B3869D}.

88. *Id.*

89. *Id.*

90. *Id.*

The Commission issued these guidelines just one week before the passage of the American Recovery and Reinvestment Act of 2009 (ARRA), which included federal funding for smart grid research and development. Through conversations with federal officials, the Commission staff learned that applications would have greater chances of success if they also obtained supporting funds from non-federal sources. Accordingly, in April 2009 the Commission invited the utilities to submit their proposals for federal funding along with any requests for rate recovery.[91] All applicants for ARRA smart grid funding were required to describe how they would design cybersecurity into new systems, and the staff effectively deferred to the judgments of federal officials in evaluating the proposals. In July, the Commission authorized several utilities to recover costs associated with specific project proposals, explaining that they "rely on the DOE criteria . . . and [they] commend the cyber security and interoperability requirements contained in [their] AMI minimum functional requirements as a reference for the utilities' final planning and design phases of their smart grid projects."[92]

Five years later, the Commission again confronted questions about cybersecurity when considering Governor Andrew Cuomo's "Reforming the Energy Vision" initiative.[93] Spurred by the infrastructural weaknesses demonstrated during Hurricane Sandy, the vision essentially affirmed and accelerated efforts to develop a smart electrical grid. It emphasized using IT to create market-based incentives for increasing the integration of distributed energy resources (DER) into the grid. This increased the importance of distributed energy resource suppliers (DERS), organizations that provided a wide range of resources, such as demand response (i.e., reducing electricity demand at times of peak usage), distributed generation and storage, and more. And it also raised questions about how the Commission should exercise oversight over a growing number of actors.

In 2014, the Commission opened a proceeding to consider its oversight responsibilities under "Reforming the Energy Vision," and the following year

91. Letters were sent on April 2, 2009 and can be found in the docket for American Recovery and Reinvestment Act of 2009 - Utility Filings for New York Economic Stimulus, No. 09-E-0310 (N.Y. Pub. Serv. Comm'n), http://documents.dps.ny.gov/public/MatterManagement/CaseMaster.aspx?MatterCaseNo=09-E-0310.

92. Order Authorizing Recovery of Costs Associated with Stimulus Projects at 39, American Recovery and Reinvestment Act of 2009 - Utility Filings for New York Economic Stimulus, No. 09-E-0310 (N.Y. Pub. Serv. Comm'n July 27, 2009), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={60420742-E365-4DF5-8499-2F578BF4A74F}.

93. REFORMING THE ENERGY VISION (REV), www.rev.ny.gov (last visited Feb. 28, 2020).

it initiated a proceeding to consider oversight of DERS.[94] Both of these proceedings acknowledged the increased challenges for cybersecurity. In a 2015 ruling, the Commission noted, while most cybersecurity standards had been developed for generation and transmission assets, the increased integration of DER presented increased risks to distribution systems. Furthermore, it noted:

> There is no single set of security standards that we can simply direct utilities to comply with. It is unlikely that any definitive set of standards will ever exist, given the dynamic nature of the threat. . . . [S]ecurity methods, systems and protocols will always require constant vigilance and reassessment, with new vulnerabilities being discovered and exploited, and new countermeasures developed and implemented.[95]

While acknowledging that most efforts at cybersecurity focused on the bulk electric system, the Commission nonetheless highlighted smart grid standards developed by NIST. Ultimately, it chose not to issue new standards, citing "the many other efforts going on within the industry and . . . the constantly evolving nature of both the system and the threats."[96] Instead, it continued to evaluate the utilities' readiness based on existing standards, and it gave utilities the "primary responsibility for ensuring that DER providers selling services into the DSP [(Distributed System Platform)] are in compliance with all applicable standards."[97] However, this guideline soon brought the utilities into conflict with ESCOs, EDIs, and other companies using electricity data.

A. CYBERSECURITY STANDARDS IN DISPUTE

On March 29, 2018, an Electronic Data Interchange (EDI) platform provided by Energy Services Group LLC and in use by Energy Transfer Partners—a company operating pipelines for gas, oil, and related

94. These were respectively Reforming the Energy Vision, No. 14-M-0101 (N.Y. Pub. Serv. Comm'n), http://documents.dps.ny.gov/public/MatterManagement/CaseMaster.aspx?MatterCaseNo=14-M-0101; and Regulation and Oversight of Distributed Energy Resource Providers and Products, No. 15-M-0180 (N.Y. Pub. Serv. Comm'n), http://documents.dps.ny.gov/public/MatterManagement/CaseMaster.aspx?MatterCaseNo=15-M-0180.

95. Order Adopting Regulatory Policy Framework and Implementation Plan at 100, Reforming the Energy Vision, No. 14-M-0101, (N.Y. Pub. Serv. Comm'n Feb. 26, 2015), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={0B599D87-445B-4197-9815-24C27623A6A0}.

96. *Id.*

97. *Id.* at 101.

commodities—was hacked.[98] Energy Transfer Partners was able to continue its operations by "handling all scheduling in house," and resumed use of the platform on April 2nd.[99] However, five major utilities in New York—Central Hudson Gas and Electric, Consolidated Edison Gas and Electric, NYSEG, RG&E, Niagara Mohawk (d/b/a National Grid), and National Fuel Gas Distribution Corporation—were also using the EDI to communicate with energy service companies. When they learned of the breach—somewhat belatedly—they immediately stopped using the platform and demanded that Energy Services Group provide information about the security of its systems, test them again for security, and sign an agreement to undertake certain measures to improve security, including purchasing cybersecurity insurance.[100]

Each of these utilities also demanded that Energy Service Entities (ESEs)—a broad category which included ESCOs, Distributed Energy Resource providers, EDI providers, Direct Customers, and New York State organizations such as New York Power Authority (NYPA)—enter into a Digital Services Agreement (DSA) with each utility. In addition to an agreement related to the confidentiality of data, some of the utilities' DSAs included a set of cybersecurity requirements and an associated vendor risk assessment, which the utilities had already been using to determine whether their contractors were implementing appropriate security controls.[101]

However, ESCOs and many other organizations objected that they did not pose the same risks to the utilities as did their vendors, and that the DSA was inappropriate. Importantly, the ESCOs cited NIST standards, arguing that the DSA failed to account for the different levels of risk posed by specific entities. For instance, a group joining forces as "the ESCO Coalition" quoted from the NIST Cybersecurity Framework, stating that the Framework was "not designed 'as a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure,' " and instead recognized that

98. Doug Olenick, *Update: Cyber-Attack knocks US Energy Services Group Offline,* SC MEDIA UK (Apr. 9, 2018), https://www.scmagazineuk.com/update-cyber-attack-knocks-us-energy-services-group-offline/article/1472917.

99. Ryan Collins & Meenal Vamburkar, *Cyber Attack Shuts Pipeline Data System, Energy Transfer Says*, WORLD OIL (Apr. 2, 2018), https://www.worldoil.com/news/2018/4/2/cyber-attack-shuts-pipeline-data-system-energy-transfer-says.

100. Joint Utilities DSA Petition at 8–9, Regulation and Oversight of Distributed Energy Resource Providers and Products, No. 15-M-0180 (N.Y. Pub. Serv. Comm'n Feb. 4, 2019), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={6F6929DD-DC16-45C8-AD41-14B2609B34BE}.

101. The DSA was based upon one previously approved by the Commission for Community Choice Aggregation (CCA) programs, with three significant additions: a data security rider with requirements for cybersecurity, a self-attestation form, and a requirement for the energy service entities to purchase cybersecurity insurance. *Id.* at 9.

> [o]rganizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They will also vary how they customize practices described in the Framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent.[102]

Accordingly, they argued that the utilities should not "have the power to unilaterally dictate specific security measures without first showing that the proposed requirements are appropriately tailored to the risk."[103] They argued that allowing the utilities "to unilaterally dictate specific security measures creates an unfair potential that the Joint Utilities will transfer a disproportionate amount of cyber risk to ESCOs and other market participants."[104] For example, ESCOs were particularly opposed to the proposed requirement that they and any third-party representatives purchase cybersecurity insurance with minimum liability limits of $10 million per event and annually.[105] They argued that any insurance requirement "should be based not on any arbitrary amount (as is the current $10 million requirement), but instead should be based on an assessment of the actual risks faced by each ESCO."[106] They also noted that the requirement "likely would make it impossible for ESCOs to deal with many third-parties, resulting in less competition and unnecessarily increased costs for consumers."[107]

Rather than taking a strong position on how national standards should be interpreted, the Commission's cybersecurity experts attempted to facilitate a business-to-business dialogue. On May 31, 2018, the Department of Public Service staff held a stakeholder meeting between the five utilities (which came to be known as the "Joint Utilities"), representatives of the energy service companies, EDI providers, and some DERS.[108] Over the next week, the utilities revised the five separate DSAs and associated risk assessments into a single uniform DSA and Self Attestation Form in which the entities were to affirm that they had implemented particular security controls. In early June, they circulated the revised forms requesting additional comment by June 22,

102. Comments of the New York Retail Choice Coalition and Supporting ESCOs on Proposed Data Security Agreement and Proposed Self-Attestation Form at 5, Cyber Security Protocols and Protections in the Energy Market Place, No. 18-M-0376 (N.Y. Pub. Serv. Comm'n June 22, 2018), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={9EB7F160-3AF6-483F-A5A7-23DFCD94005A}.

103. *Id.* at 7.

104. *Id.*

105. *Id.* at 3.

106. *Id.* at 12.

107. *Id.* at 10.

108. *Id.* at 1.

2018, but mandating the signing of the Self-Attestation Form by the end of June. In the meantime, on June 14th, the NYPSC initiated a proceeding on Cybersecurity Protocols in the Marketplace, directing its staff to monitor the business-to-business discussions and report back to the Commission by the end of the summer.[109]

However, there was no speedy resolution to the conflict over appropriate security requirements. Two additional days of technical conferences on July 26–27, 2018, yielded some progress, as did a follow-up conference call on August 1st. Nonetheless, many ESCOs requested further discussions, arguing that substantial problems remained. The utilities, however, argued that there was not enough time for further conversation, as they needed to reach closure by the end of the month to comply with the Commission's order. Accordingly, the utilities circulated a revised draft of the Self-Attestation Form on August 2nd, and a revised DSA on August 16th, mandating that they be signed by August 24th and 31st, respectively. As they emphasized in subsequent filings, the revised Self-Attestation Form consisted of sixteen security controls drawn from NIST standards for critical infrastructure security.[110] Accordingly, they argued that these represented a reasonable set of minimum standards.[111]

B. CALLS FOR MORE EXPERT DIALOGUE

However, the ESCOs and related companies continued to highlight problems with the requirements. At stake was not only whether the security requirements proposed by the utilities were an appropriate interpretation of national standards was at stake, but whether they were feasible. For instance, the self-attestation form required that data be encrypted in transit, but the companies noted that this was "impossible for unknown third-parties."[112] Although the companies continued trying to resolve various issues before the August deadlines mandated by the utilities, they failed to reach an agreement. Some companies signed under protest, while others refused to sign.

---

109. *See* Order Establishing Minimum Cybersecurity and Privacy Protections and Making Other Findings at 5, Regulation and Oversight of Distributed Energy Resource Providers and Products, No. 15-M-0180 (N.Y. Pub. Serv. Comm'n Oct. 17, 2019), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={99401E73-404B-4A4B-A0CA-6C2585DB7EFF}.

110. *See id.* at 6.

111. *See id.* at 7.

112. Comments of New York Retail Choice Coalition and Supporting ESEs in Opposition to Joint Utilities Petition for a Declaratory Ruling at 11, Cyber Security Protocols and Protections in the Enegery Market Place, No. 18-M-0376 (N.Y. Pub. Serv. Comm'n Nov. 30, 2018), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={4D20690A-1619-4DBD-846F-B986734AA6B1}.

The companies objected to the utilities' requirements and the process of negotiating those requirements, arguing that additional negotiation among experts was necessary. As early as June, Starion Energy argued that "the DSA fails to serve the Commission's worthy objective of data security protection. . . . [T]he DSA needs to be entirely reconceived, not merely redrafted, and a broader group of industry and technical experts needs to be engaged in the process."[113] In August and September, several companies and coalitions of companies called for the Commission to establish a cybersecurity working group akin to what had earlier been established for EDI.[114] Thus, by the end of the summer, the Commission's experts had neither resolved the technical challenges posed by the proposed requirements, nor ensured that a satisfactory level of expert dialogue occurred in the business-to-business process.

The Commission staff's report on the business-to-business process, filed in September, did little to ameliorate these grievances. The report commended the dialogue as "a nimble process by which the parties could develop cyber protections that address the significant concern facing New York's distribution utilities," and concluded that "the revised DSA strikes a fair balance between the Joint Utilities' concerns of both protecting the utility systems from infiltration and against customer data breaches, and the ESEs' concerns of overreaching and over-burdensome cyber security requirements."[115] They noted that roughly eighty percent of ESCOs had executed the DSA, and seventy-five percent had executed the Self-Attestation. Additionally, about half of the EDI providers had executed the DSA, and only about thirty-five percent had executed the Self-Attestation. They further stated that most of the "active ESEs that have not complied with the August deadlines or filed under protest,

113. Initial Comments of Starion Energy, Inc. at 2, Cyber Security Protocols and Protections in the Energy Market Place, No. 13-M-0376, (N.Y. Pub. Serv. Comm'n June 22, 2018), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={B1D2F816-6D9D-4723-A139-32D731703F4D}.

114. Retail Energy Supply Association's Motion to Form a Cybersecurity Working Group, Cyber Security Protocols and Protections in the Energy Market Place, No. 18-M-0376 (N.Y. Pub. Serv. Comm'n Aug. 28, 2018), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={D5E5B0A7-F775-45AB-9AB5-C972D2AB5B8E}; Final Comments of DSA Coalition Members on Proposed Data Security Agreement and Proposed Self-Attestation, Cyber Security Protocols and Protections in the Energy Market Place, No. 18-M-0376 (N.Y. Pub. Serv. Comm'n Sept. 24, 2018), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={679B4AFE-20E8-459C-A4E3-3BD9C9A4451F}.

115. Staff Report on the Status of the Business-to-Business Collaborative to Address Cyber Security in the Retail Access Industry at 3, Cyber Security Protocols and Protections in the Energy Market Place, No. 18-M-0376 (N.Y. Pub. Serv. Comm'n Sept. 24, 2018), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={46C17240-E3D1-4088-B45E-9E04C5A5886F}.

have not fully articulated the basis for not complying."[116] They speculated that this was because of the lack of Commission action, as well as what they called "inadequate justification for cyber insurance"—yet they did not recommend eliminating that justification.[117]

Despite tilting towards the utilities' position, in one sense the staff validated the ESEs' argument that security requirements should be tailored to the risks of the organization. It noted, for example, that "some DERS utilize different forms of electronic communication with the utilities and/or may receive different customer data points as compared to an ESCO."[118] Accordingly, it recommended establishing a business-to-business process for DERS and went on to facilitate multiple stakeholder meetings on this topic.[119] But overall, the staff report attempted one kind of closure—accepting the terms of the DSA and self-attestation—while acknowledging that requirements could never be entirely finalized. They noted calls for the Commission to establish a working group to discuss cybersecurity requirements and expressed support for such a group as a means of adapting the requirements "to an everchanging cyber landscape going forward."[120]

The utilities were emboldened by the staff report, citing its conclusions about the quality of the proceedings and fairness of the resulting requirements. Frustrated by what they viewed as the intransigence of the organizations refusing to sign the DSA, in November 2018, the utilities petitioned the Commission to rule that they could disconnect organizations from accessing their systems if they refused to sign the DSA and meet other security standards.[121]

However, ESEs protested, reiterating the problems with the DSA and objecting to the process by which it was drafted. For example, the Retail Energy Supply Association (RESA) objected to the staff's conclusion that the business-to-business process had been fair and produced a "balanced DSA," arguing that, "because of the superior bargaining power held by the Joint Utilities, the agreements provide the Joint Utilities with a significant amount

116. *Id.* at 5.

117. *Id.* at 6.

118. *Id.* at 8.

119. *See* Order Establishing Minimum Cybersecurity and Privacy Protections and Making Other Findings, *supra* note 109, at 5–6.

120. Staff Report on the Status of the Business-to-Business Collaborative to Address Cyber Security in the Retail Access Industry, *supra* note 115, at 7.

121. *See* Petition of the Joint Utilities for Declaratory Ruling, Retail Access Business Rules, No. 98-M-1343 (N.Y. Pub. Serv. Comm'n Nov. 9, 2018), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={13DAEE84-EF37-49D9-A67B-BCE38A46C041}.

of control over their ESCO competitors."[122] They continued to object to a number of provisions, including the utilities' assertion of the right to audit the ESCOs and the imposition of the cybersecurity insurance requirement, for the same reasons discussed above.

The Joint Utilities responded to such criticism by petitioning the Commission to affirm the business-to-business process and their right to require that the ESE's comply with several minimum standards, including requirements that the industry continued to dispute, such as purchasing cybersecurity insurance.[123] However, the ESCOs continued to object to the process, their objections being both what they saw as the superior bargaining power of the utilities and the lack of full and open dialogue among technical experts. The Mission:Data coalition went so far as to accuse the utilities of acting in bad faith, stating that they "seek to exploit the current climate of fear surrounding cybersecurity risks in order to inappropriately seize certain powers over distributed energy resource ("DER") suppliers."[124] The DSA coalition argued:

> The business-to-business process utilized thus far to develop the DSA and SAF was neither fair nor reasonable, because ESE's have always been under threat of repercussions by the Joint Utilities for not signing these agreements. Moreover, the Joint Utilities have virtually excluded any interactive dialogue between the respective information technology experts of ESEs and the Joint Utilities on the DSA and SAF, except for a single two-hour call on August 1, 2018, which only came about after vociferous complaints . . . of the Joint Utilities' non-responsiveness for weeks to repeated ESE requests for such integral, technical dialogue.[125]

122. Retail Energy Supply Association's Response to the Joint Utilities Petition for Declaratory Ruling at 3, Cyber Security Protocols and Protections in the Energy Market Place, No. 18-M-0376 (N.Y. Pub. Serv. Comm'n Dec. 21, 2018), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={3EDD440A-6A94-47BF-9697-C9E6189CE949}.

123. Joint Utilities DSA Petition, Cyber Security Protocols and Protections in the Energy Market Place, No. 18-M-0376 (N.Y. Pub. Serv. Comm'n Feb. 4, 2019), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={597AA41A-73AE-4C3B-8FBF-CB001F00A765}.

124. Case 18-M-0376—Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place, New York Public Service Commission, Response of Mission:data Coalition to the Commission's February 20, 2019 Notice Soliciting Comments at 2 (Apr. 29, 2019), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={07F2522E-390B-4669-939A-C05FCE80CF34}.

125. DSA Coalition Response to Joint Utilities II at 3, Regulation and Oversight of Distributed Energy Resource Providers and Products, No. 15-M-0180 (N.Y. Pub. Serv.

Similarly, the ESEs took issue with the findings of the Commission's experts. For example, the DSA coalition argued that the staff report "failed to recognize the Joint Utilities' superior bargaining position" and also failed to provide "independent analysis" of issues that the Commission had instructed it to address, such as vulnerabilities in the Joint Utilities' systems, "whether the Joint Utilities' mandated practices under the DSA and SAF would actually protect utilities' systems and confidential and sensitive customer information," or "analysis on whether insurance is an efficient and effective vehicle for mitigating financial risks."[126]

Similarly, RESA argued that the utilities' demands would not actually reduce risk, but simply transfer risk from the utilities to the ESEs. RESA argued: "[T]he DSA is nothing more than a contractual agreement governing liability and does not actually ensure that the utility network is not compromised by EDI transactions. The DSA itself does not increase or decrease any perceived risk to a utility's system, nor does executing the agreement mitigate any such perceived risk."[127]

The ESE's continued to raise questions about technical feasibility which could only be assessed by technical experts. For instance, they objected that some of the requirements—such as encrypting all data in transit—were not technically feasible for some kinds of communication, such as email communications with customers.[128]

Thus, by the spring of 2019, the Commission was failing to perform cybersecurity expertise. The problem was not that the Commission did not have access to knowledgeable and skilled individuals; the technical competence of the Commission's security team was not in question. Rather, the problem was that the Commission's experts were unable to forge a public consensus about what cybersecurity measures should be required of ESEs. This was largely because they were unable to facilitate an adequate level of dialogue among experts in different sectors of the industry, as demonstrated by the growing mistrust between the ESEs and the utilities.

In this context, the Commission staff could no longer simply defer to the experts in the industry, in particular the utility industry.

Comm'n Apr. 29, 2019), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={969DBFB3-F1B3-4BB9-84CF-E0BD298138CF}.

126. *Id.* at 8.

127. Retail Energy Supply Association's Response to the Joint Utilities ESE Petition at 10, Cyber Security Protocols and Protections in the Energy Martket Place, No. 18-M-0376 (N.Y. Pub. Serv. Comm'n Apr. 29, 2019), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={AF7FB9AE-0113-4CBA-96D3-349ED01A8DE5}.

128. *See* DSA Coalition Response to Joint Utilities II, *supra* note 119, at 13–14.

C. FINAL RULING

The Commission attempted to strike this balance on October 17, 2019, when it finally issued an "Order Establishing Minimum Cybersecurity and Privacy Protections and Making other Findings."[129] The order grounded its epistemic authority in cybersecurity standards such as those promulgated by NIST, by accepting the argument that cybersecurity requirements should be based upon risks. It distinguished between risks to the misuse of data and risks to information systems. Further, it noted that some organizations did not pose the same level of risk to information systems. Accordingly, while the Commission required nearly all of the ESEs to implement appropriate protections to protect customer privacy, it ruled that "only entities that electronically receive or exchange customer information from a direct connection with the utilities' IT systems, except by email, will need to adopt the cybersecurity requirements established in [the] Order."[130]

The Commission also acknowledged technical feasibility concerns raised by the ESEs, for example by exempting email communications from requirements that all confidential customer information be encrypted in transit. The Commission also allowed the utilities to require audits but ruled that such audits must be conducted by a third party rather than the utilities, as originally proposed, a provision which raised concerns about the protection of proprietary information. And perhaps in the biggest triumph for the ESEs, the Commission ruled that the organizations would not be required to purchase cybersecurity insurance.[131] The Commission ruled that "a cybersecurity insurance requirement, which is mainly intended to address damages after an incident occurs," would not reduce risk and "would serve to act as little more than a market barrier to entry."[132]

This order appears to have salvaged what was nearly a failed performance of expertise. The Mission:Data coalition praised the ruling as "a big win for innovation" and highlighted several aspects of the DSA and self-attestation form that the Commission had rejected.[133] The utilities moved forward with revising the forms as directed by the Commission. In the context of this increasingly competitive and fractious industry, performing cybersecurity

129. *See* Order Establishing Minimum Cybersecurity and Privacy Protections and Making Other Findings, *supra* note 109.

130. *Id.* at 36.

131. *Id.* at 58.

132. *Id.*

133. Robert Walton, *New York Adopts Utility-ESCO Cybersecurity Standards, Rejects Insurance Requirements*, UTILITY DIVE (Oct. 18, 2019), https://www.utilitydive.com/news/new-york-adopts-utility-esco-cybersecurity-requirements-rejects-insurance/565333/.

expertise required that the Commission's staff make detailed judgments about how to balance security against other goals, such as innovation and the integration of renewable energy resources.

VI. CONCLUSION

As the cases discussed above demonstrate, state and local regulators do not merely face the challenge of sourcing expertise; they must also help to perform authoritative expertise in a rapidly evolving technological landscape where consensus is often nowhere to be found. The New York Public Services Commission was very proactive about hiring both consultants and in-house experts in the wake of 9/11. Yet, performing cybersecurity expertise required more than simply hiring people; it also entailed making authoritative assessments of various proposals for improving cybersecurity, assessments which entailed balancing goals such as security, innovation, affordability, and more. This was no easy feat.

By most measures, the Commission's cybersecurity staff have successfully performed expertise. They have articulated cybersecurity standards that the electric sector has largely accepted, and there is little evidence that members of the public question the security assurances offered by the Commission, even after public breaches. While security is difficult, if not impossible, to measure, there is every reason to believe that the Commission's experts have improved security at the regulated utilities. But understanding how the Commission's experts have improved security requires attending to more than just hiring practices; it also requires analysis of how the Commission's experts cultivate relationships with the regulated utilities, related companies, and the artifacts that they seek to secure.

This Article has highlighted at least three contexts in which the Commission's staff cultivate these relationships. First, the Commission's experts have been called upon to investigate security breaches. In these contexts, they have typically highlighted best practices and industry standards By critiquing companies for failing to implement best practices and standards, the staff reinforce the notion that they possess the specialized knowledge and skills needed to avoid breaches in the future, and thereby enhance their own authority, even in the face of evidence that oversight has failed.

Second, the Commission's experts are often called upon to assess the legitimacy of requests to recover the costs of new cybersecurity initiatives. Here again, they often invoke standards and best practices, yet the implementation of standards often leaves much to the discretion of organizations. In everyday rate cases, ambiguities about how to apply standards are generally not discussed. Instead, both the utilities' and the Commission's

cybersecurity experts generally appear to agree on the need for specific investments, and both emphasize the need to keep pace with rapidly changing threats. The near-universal convergence of the Commission's experts and the utilities' experts suggest that a process of tacit coordination is likely at work. Ultimately, a substantial part of the Commission's experts' job is to maintain ongoing dialogue with the industry. Indeed, NARUC's recent guidelines note that "[a]s a regulator, if you can engage with the companies on [cybersecurity] informally, as a discrete issue separated from the baggage of a regulatory proceeding, you're likely to get better information."[134] This is particularly important in the context of cybersecurity, where the traditional regulatory emphasis on transparency may need to be balanced against the demands of security. The key point of this Article is that ongoing contact between the Commission's and utilities' experts not only allows for oversight, but it also allows for the coordination of cybersecurity planning behind closed doors, minimizing the potential for public disagreement about how to interpret and apply standards. This then enhances the authority of the Commission's expert recommendations.

However, the Commission's experts were unable to refer to best practices or coordinate planning behind closed doors in the third context discussed here: helping to adjudicate standards for a rapidly changing and divided industry. Although the Commission's experts attempted to simply facilitate the negotiation of cybersecurity requirements for organizations accessing utility data, they ultimately were forced to make specific recommendations to the Commission. These recommendations entailed judgments about not only technical feasibility, but also about how to balance security requirements against the desire to lower barriers to entry in a new and rapidly growing market for energy services. Performing cybersecurity expertise ultimately required more than just knowledge. It entailed earning trust in an increasingly competitive industry.

134. KEOGH & THOMAS, *supra* note 4, at 18.